Pengamanan Dokumen Teks Dengan Menerapkan Kombinasi Algoritma Kriptografi Klasik

Leo Dearman Simatupang[1], Khairil*[2]
[1,2] Universitas Dehasen Bengkulu; Jalan Meranti Raya No. 32 Sawah Lebar Bengkulu
Email : [1]leodearmans@gmail.com , [2*]khairil@unived.ac.id

Abstrak

Keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu data, pesan dan informasi. Vigenere Cipher bekerja dengan membaca kata per karakter, dimana apabila pesan yang dikirim melebihi panjang kunci yang digunakan, maka kunci akan diulang kembali sampai pesan yang dikirim tersebut mendapatkan kunci masing-masing. Caesar Cipher melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama. Dengan mengkombinasikan algoritma Vigenere Cipher dan Caesar Cipher tersebut menghasilkan sebuah metode yang dapat memberikan tingkat keamanan yang lebih baik dibandingkan dengan penerapan masing – masing metode tersebut secara terpisah. Hasil dari analisa dan pengujian yang dilakukan dengan menggunakan kunci dekripsi yang berbeda menghasilkan chiperteks tidak dapat dikembalikan yang mana menunjukkan hal yang normal dikarenakan metode yang digunakan merupakan kriptografi simetris sehingga proses dekripsi hanya bisa dilakukan menggunakan kunci yang sama dengan kunci pada saat dekripsi.

Kata Kunci : Keamanan, Vigenere Cipher, Caesar Cipher

Abstract

Security and confidentiality are one of the important aspects of data, messages and information. Vigenere Cipher works by reading word per character, where if the message sent exceeds the length of the key used, the key will be repeated until the message sent gets its respective key. Caesar Cipher shifts all characters in plaintext with the same shift value. By combining the Vigenere Cipher and Caesar Cipher algorithms, it produces a method that can provide a better level of security than the application of each method separately. The results of the analysis and testing carried out using different decryption keys resulted in the ciphertext being non-refundable, which shows that it is normal because the method used is symmetric cryptography so that the decryption process can only be carried out using the same key as the key at the time of decryption.

Keywords: Security, Vigenere Cipher, Caesar Cipher

1. Pendahuluan

Data merupakan salah satu asset terpenting yang perlu dilindungi karena tidak menutup kemungkinan data tersebut dapat bocor ataupun dicuri oleh orang yang akan menyalahgunakan data. Terkait dengan keamanan data menimbulkan tuntutan akan tersedianya suatu sistem pengamanan data yang lebih baik agar keamanan data terhindar dari berbagai ancaman yang mungkin akan terjadi.

Aplikasi yang banyak dipakai saat ini telah menerapkan terhadap pengamanan data, seperti pengamanan pada aplikasi komunikasi (chatting), pengamanan pada transaksi *e-commerce*, sehingga pada transaksi perbankan. Masing – masing aplikasi mempunyai cara tersendiri dalam pengamanan data. Pengamanan data dengan model *end to end encryption* yang digunakan pada fitur chat atau perbankan merupakan yang untuk menjaga kerahasian data. Dengan model ini hanya pihak pengirim dan penerima yang bisa membaca dan memeriksa keaslian data yang dikirimkan pada jalur internet public.

Beberapa cara melakukan pengamanan data ataupun pesan, diantaranya dengan menggunakan teknik penyamaran data dengan istilah kriptografi. Kriptografi adalah ilmu untuk mempelajari penulisan secara rahasia dengan tujuan bahwa komunikasi dan data dapat dikodekan (*encode/encrypt*) dan dikodekan (*decode/decrypt*) kembali untuk mencegah pihak-pihak lain yang ingin mengetahui isinya. Kriptografi (*Cryptography*) berasal dari bahasa

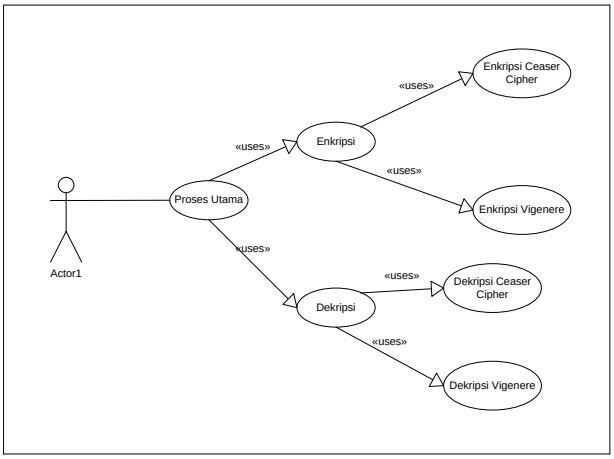
Yunani yaitu dari kata *kryptos* yang artinya tersembunyi. Kriptografi dapat diartikan sebagai tulisan yang dirahasiakan atau dapat diartikan juga sebagai suatu ilmu ataupun seni yang mempelajari bagaimana sebuah data, informasi dan dokumen dikonversi kebentuk tertentu yang sulit untuk dimengerti [8].

Metode kriptografi tersebut mempunyai teknik dan cara tersendiri. Langkah-langkah pengerjaan setiap metode berbeda-beda, baik dari segi panjang maupun kerumitan. Salah satu metode kriptografi klasik yang masih digunakan adalah sandi *Vigenère Cipher* dan *Ceasar Chiper*. *Caesar Cipher* merupakan teknik enkripsi substitusi yang pertama kali dikenal dan paling sederhana, yang ditemukan oleh Julius Caesar. Metode yang digunakan dalam *caesar cipher* ini adalah dengan mempertukarkan setiap huruf asli (*plain text*) dengan huruf lain menggunakan interval 3 sehingga membentuk suatu cipher text. Sedangkan *vigenere cipher* adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi *caesar cipher* berdasarkan huruf-huruf pada kata kunci. Sandi *vigenère cipher* merupakan bentuk sederhana dari sandi substitusi polialfabetik. Kelebihan sandi ini dibanding sandi *caesar cipher* dan sandi monoalfabetik lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi.

Demi keamanan data lebih kuat pengujian dengan kolaborasi kedua metode tersebut dikombinasikan menjadi satu, sehingga menghasilkan *cipher* data dari metode *Caesar cipher* dan vi*genere chiper*. Kinerja dari algoritma kriptografi klasik dalam proses enkripsi dan dekripsi data teks serta dibuat suatu program untuk melakukan proses enkripsi dan dekripsi data teks menggunakan *platform* Visual Studio 2010. Visual Basic (VB).Net adalah salah satu kumpulan *tools* pemrograman yang terdapat pada paket Visual Studio. Pada Visual Studio terdapat beberapa *tools* pemrograman seperti Visual C++, Visual C# dan Visual F#[6]. Lingkungan pengembangan dari Visual Basic.Net disebut juga dengan .*Net Framework*. *Framework* ini menangani bagaimana .Net programming membangun tipe intristik, *class* dan *interface* [10]

Pada penelitian yang telah dilakukan terdahulu Algoritma yang dibuat mengunakan kombinasi kunci yang sulit diperkirakan, dikarenakan menggunakan kombinasi dua kunci yang berbeda dengan Aplikasi Cryssage, aplikasi ini digunakan untuk melakukan enkripsi pesan dan mengirimnya pesan tersebut ke tujuan penerima pesan.

2. Metode Penelitian



Gambar 1. Use Case Aplikasi Kriptografi

Use Case direpresentasikan dengan urutan langkah pengguna dalam pemakaian apliksai. *Use case* diagram menggambarkan fungsionalitas yang diharapkan dari sebuah sistem. Yang ditekankan adalah "apa" yang diperbuat sistem, dan bukan "bagaimana" [1]. Sebuah *use case* merepresentasikan sebuah interaksi antara aktor dengan sistem. *Use case* merupakan sebuahpekerjaan tertentu, misalnya login ke sistem, meng-*create* sebuah daftar belanja, dan

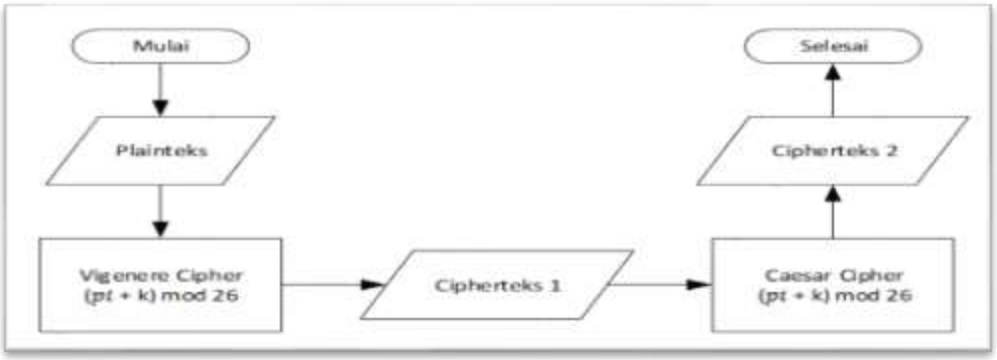
sebagainya [5]. Use Case ini menjelaskan mengenai bagaimana proses pengenkripsian dan dekripsi menggunakan kedua algoritma vigenere cipher dan ceaser cipher, untuk menyandikan dokumen yang ingin di jaga kerahasiaannya. Gambar 1 use case yang digunakan pada sistem

Dalam melakukan penelitian ini, penulis menggunakan metode terapan (*applied research*). Tujuan utama penelitian terapan adalah pemecahan masalah sehingga hasil penelitian dapat dimanfaatkan untuk kepentingan manusia baik secara individu atau kelompok.

Gambar 2. Tahapan dalam Penelitian

Identifikasi Masalah merupakan Tahap ini dirumuskan masalah yang akan menjadi objek penelitian. Perumusan masalah dilakukan pada pengamanan dokumen menggunakan Vigenere dan *Ceaser Cipher*. Penerapan Metode Vigenere dan Caesar cipher pada Tahap ini dilakukan penerapan terhadap metode *Vigenere* dan *Ceaser Cipher* pada dokumen yang dilakukan secara manual dimana proses pembangkitan kunci, enkripsi dan dekripsi pada dokumen dihitung secara bertahap untuk menganalisa proses komputasi dari metode *Vigenere* dan *Ceaser Cipher* sehingga dapat membantu dalam membangun aplikasi atau sistem yang akan digunakan dalam mengamankan dokumen. Perancangan Sistem pada Tahap ini dilakukan perancangan sistem pengamanan dokumen Proses pembangkitan kunci, enkripsi dan dekripsi serta tahap – tahapnya dirancang antarmuka. Implementasi dan Pengujian pada tahap pengamanan dokumen menggunakan metode *Vigenere* dan *Ceaser Cipher*. Selanjutnya dilakukan pengujian dengan melakukan percobaan enkripsi dan dekripsi terhadap beberapa dokumen pengujian untuk memperoleh validasi terhadap fungsional dan keluaran dari aplikasi. Analisa Hasil Keluaran pada tahap ini menganalisa dan mengamati bagaimana hasil keluaran dari aplikasi yang dibangun. Adapun keluaran yang diamati pada kegiatan ini adalah keluaran dari proses enkripsi dan dekripsi dari aplikasi yang dibangun. Pada hasil enkripsi akan diamati apakah dokumen hasil enkripsi tidak dapat dikenali lagi atau tidak lagi sama dengan dokumen aslinya, sedangkan pada dokumen hasil dekripsi diamati untuk memastikan bahwa dokumen hasil dekripsi harus sesuai dengan dokumen asli sebelum dienkripsi. Kesimpulan pada tahap ini dilakukan penyusunan kesimpulan diperoleh dari kegiatan

Berikut ini akan digambarkan flowchart proses enkripsi algoritma Vigenère cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1986. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenère, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku La Cifra del Sig. Giovan Batista Belaso, sebuah buku yang ditulis oleh Giovan Batista Belaso [6]. Vigenere Vigenere cipher adalah metode mengenkripsi teks alfabet dengan menggunakan serangkaian caesar cipher yang berbeda berdasarkan huruf dari kata kunci dan merupakan bentuk substitusi polyalphabetic yang sederhana. Karakter yang digunakan dalam Vigenere Cipher yaitu A, B, C, ..., Z dan dikonversi kedalam angka 0, 1, 2, ..., 25. Proses enkripsi dilakukan dengan menulis kunci berulang kali sesuai dengan panjang karakter pada pesan [8] Vigenere Cipher juga dapat menggunakan sebuah tabel untuk menengkripsikan sebuah plaintext yang mana tabel tersebut terdiri dari 26 baris dan kolom alphabet, dan tiap barisnya akan digeser satu huruf ke kiri [4]



Gambar 3. Proses enkripsi kombinasi vigenere cipher dan Caesar cipher

Dan Ceasar Cipher Algoritma kriptografi yang mula-mula digunakan oleh kaisar Romawi, Julius Caesar (sehingga dinamakan juga caesar chiper), untuk menyandikan pesan yang ia kirim kepada para gubernurnya. Caranya adalah dengan mengganti (menyulih atau mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet) [2] Caesar Cipher adalah menentukan besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks, Menukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya [3].

Enkripsi : $E(p_i) = (p_i + key)\ mod\ 26$

Dekripsi : $D(c_i) = (c_i - key)\ mod\ 26$

Metode Algoritma *Vigenere* dan *Ceaser Cipher* yang akan di implementasikan pada pesan teks.

1. Vigenere

Plainteks : KRIPTOGRAFI
Key : DEHASEN

PLAINTEKS	K	R	I	P	T	O	G	R	A	F	I
Posisi Abjad	10	17	8	15	19	14	6	17	0	5	9
KEY	D	E	H	A	S	E	N	D	E	H	A
Posisi Abjad	3	4	7	0	18	4	13	3	4	7	0
(P+KEY)mod 26	13	21	15	15	11	18	19	20	4	12	9
CIPHER TEKS	N	V	P	P	L	S	T	U	E	M	I

2. Ceasar Cipher

Plainteks : NVPPLSTUEMJ
Key : 15

PLAINTEKS	N	V	P	P	L	S	T	U	E	M	J
KEY CEASAR	15	15	15	15	15	15	15	15	15	15	15
(P+KEY)mod 26	2	10	4	4	0	7	8	9	19	1	24
CIPHER TEKS	C	K	E	E	A	H	I	J	T	B	X

Dekripsi

1. Vigenere

CIPHER TEKS	C	K	E	E	A	H	I	J	T	B	X
Posisi Abjad	2	10	4	4	0	7	8	9	19	1	24
KEY	D	E	H	A	S	E	N	D	E	H	A
Posisi Abjad	3	4	7	0	18	4	13	3	4	7	0
(C-KEY)mod 26	-1	6	-3	4	-18	3	-5	6	15	-6	24
PLAINTEKS	Z	G	X	E	I	D	V	G	P	U	X

2. Ceasar Cipher

CIPHER TEKS	Z	G	X	E	I	D	V	G	P	U	X
Posisi Abjad	25	6	23	4	8	3	21	6	15	20	24
KEY	15	15	15	15	15	15	15	15	15	15	15
(C-KEY)mod 26	10	17	8	15	19	14	6	17	0	5	9
PLAINTEKS	K	R	I	P	T	O	G	R	A	F	I

3. Hasil dan Pembahasan

3.1. Hasil

Aplikasi pengamanan data teks dengan menerapkan algoritma kriptografi klasik dalam pengamanan dokumen dibangun sesuai dengan analisa dan perancangan. Hasil dari aplikasi yang dibangun serta pengujian yang telah dilakukan dapat aplikasi ini digunakan dalam mengamankan pesan yang terenkripsi dengan dua metode. sehingga dalam pengembalian data ke aslinya hanya dapat dilakukan menggunakan kunci yang sama pada saat kunci *enkripsi*.

3.2. Pembahasan

Pada aplikasi ini terdapat beberapa *interface* atau antarmuka yang di desain untuk mempermudah *user* dalam menggunakan aplikasi.

Gambar 4. Halaman Utama Aplikasi

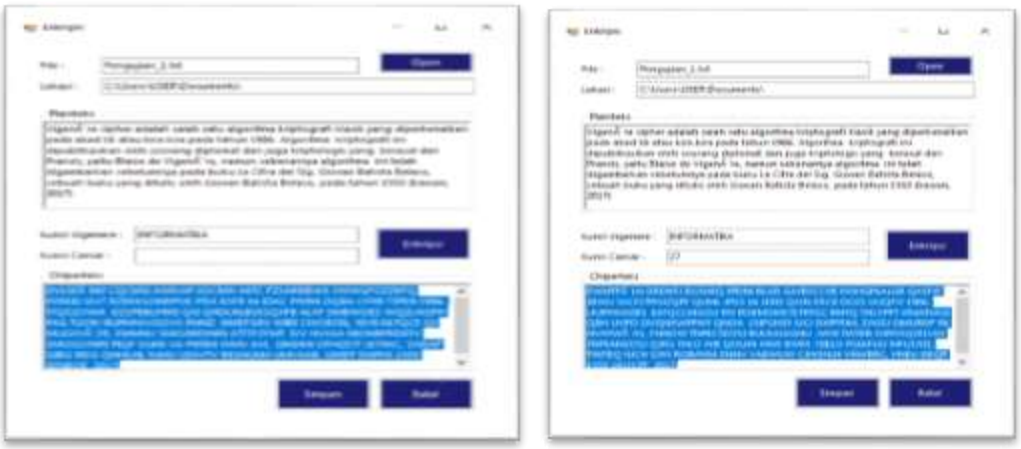
Pada menu utama terdapat menu enkripsi untu proses mengenkripsi pesan, menu dekripsi untuk mengembalikan ke pesan semula. Untuk melakukan enkripsi pesan plainteks dibuka selanjutnya pengguna dapat melakukan proses enkripsi dengan memasukkan kunci yang telah dibangkitkan sebelumnya dan melakukan proses enkripsi dengan menekan tombol "Enkripsi" sehingga proses enkripsi dilakukan dan akan menampilkan chiperteks seperti yang terlihat pada gambar 5

Gambar 5. Enkripsi data teks

Chiperteks hasil enkripsi kemudian disimpan menjadi file menggunakan tombol "Save" sehingga file *cipherteks* tersebut dapat di dekripsi kembali menggunakan *form dekripsi*. Berkas *chiperteks* dibuka dengan menggunakan tombol "Open" pada menu dekripsi akan menampilkan dialog untuk memilih *file chiperteks* yang akan di dekripsi. Seperti pada gambar 6.

Gambar 6. Dekripsi data teks

Pengujian enkripsi dan dekripsi kunci yang sama adalah pengujian yang mana proses enkripsi dan dekripsi menggunakan kunci yang sama. Pengujian menggunakan plainteks pengujian seperti yang telah disebutkan sebelumnya adapun pengujian menggunakan kunci Vigenere Cipher "INFORMATIKA" dan kunci Ceaser Chiper "27" terlihat pada gambar 7.

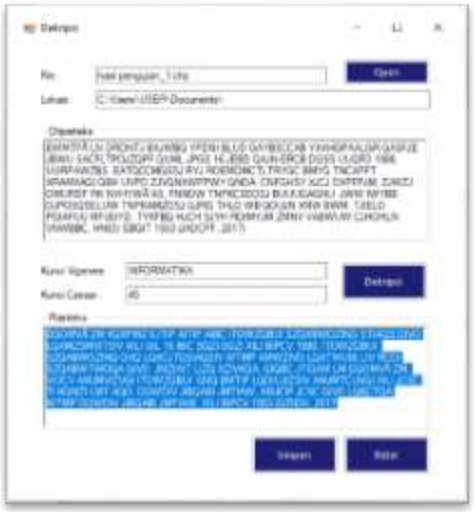


Gambar 7 Proses Enkripsi Vigenere Cipher dan Ceasar Cipher

Dilanjutkan dengan melakukan dekripsi terhadap chiperteks yang dihasilkan pada gambar 8

Gambar 8 Proses Dekripsi Vigenere Cipher dan Ceasar Cipher

Pengujian enkripsi dan dekripsi kunci yang merupakan pengujian yang mana proses dekripsi menggunakan kunci yang berbeda. Pengujian menggunakan plainteks pengujian menggunakan kunci "INFORMATIKA" untuk dekripsi vigenere cipher dan "45" dekripsi Ceasar Cipher, hasilnya seperti pada gambar 8.



Gambar 8. Hasil Proses Dekripsi Dengan Kunci Ceasar Cipher Beda

Pengujian dekripsi pesan kunci vigenere cipher yang beda adalah pengujian untuk melihat pengaruh kunci yang berbeda pada plainteks yang sama. Pengujian menggunakan plainteks pengujian menggunakan kunci "27" untuk Ceaser Cipher dan menggunakan kunci vigenere cipher yang berbeda "BENGKULU", hasilnya pada gambar 9.

Gambar 9. Hasil Proses Dekripsi Dengan Kunci Vigenere Cipher Beda

4. Kesimpulan

Pengamanan data teks dengan menerapkan algoritma kriptografi klasik *Vigenere Cipher* dan *Ceasar Cipher* dalam pengamanan dokumen dapat dikombinasikan dengan baik sesuai dengan kedua metode. Proses enkripsi dimulai terlebih dahulu menggunakan metode *Vigenere Cipher* yang kemudian hasil enkripsi tersebut di enkripsi lagi menggunakan metode *Ceasar Cipher* sehingga seperti proses enkripsi beruntun. Proses dekripsi merupakan proses kebalikan dari proses dekripsi sehingga plainteks dapat diperoleh kembali. Implementasi kedua metode tersebut menghasilkan sebuah metode yang dapat memberikan tingkat keamanan yang lebih baik dibandingkan dengan penerapan masing – masing metode tersebut secara terpisah.

Dari hasil pengujian yang telah dilakukan aplikasi yang dikembangkan dapat bekerja sesuai dengan yang diharapkan. Pengujian normal menghasilkan chiperteks dan plainteks yang sesuai. Pengujian enkripsi dan dekripsi menggunakan kunci yang berbeda untuk melihat fungsi aplikasi jika diberikan kunci yang tidak sama pada saat proses enkripsi dengan dekripsi. Dari pengujian yang dilakukan chiperteks tidak dapat dikembalikan yang mana menunjukkan hal yang normal dikarenakan metode yang digunakan merupakan kriptografi simetris sehingga proses dekripsi hanya bisa dilakukan menggunakan kunci yang sama dengan kunci pada saat dekripsi Dari hasil aplikasi ini dilakukan pada perangkat lunak ini dapat digunakan oleh pengguna umum untuk mengamankan pesan.

Daftar Pustaka

[1] Alfina, O., & Harahap, F. (2019). Pemodelan Uml Sistempendukung Keputusan Dalam Penentuan Kelas Siswa Siswa Tunagrahita. *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi*, 143-150.

[2] Andriyanto. (2019). Implementasi Algoritma Caesar Cipher Untuk Keamanan Data Pada Kartu Ujian. *JURNAL BUFFER INFORMATIKA*, 1-7.

[3] Angriani, H., & Saharaeni, Y. (2019). Implementasi Algoritma Caesar Cipher Pada Keamanan Data Sistem E-Voting Pemilihan Ketua Organisasi Kemahasiswaan. *Inspiration : Jurnal Teknologi Informasi dan Komunikasi* , 123-126.

[4] Darmawan , M., & Windarto , W. (2018). Implementasi Algoritma Kriptografi Vigener Cipher Dan Affine Cipher Untuk Mengamankan Pesan Pada Aplikasi Chatting Berbasis Android. *SKANIKA (Sistem Komputer dan Teknik Informatika)*, 24-32.

[5] Haviluddin. (2016). Memahami Penggunaan UML (Unified Modelling Language). *Jurnal Informatika Mulawarman*, 18-29.

[6] Irawan, M. (2017). Implementasi Kriptografi Vigenere Cipher Dengan Php. *JURNAL TEKNOLOGI INFORMASI (JurTI)*, 11-21.

[7] M. Ziaurrahman, Utami, E., & Wibowo, F. (2019). Modifikasi Kriptografi Klasik Vigenere Cipher Menggunakan One Time Pad Dengan Enkripsi Berlanjut. *Jurnal Informasi Interaktif*, 63-68.

[8] Mendrofa, E., Purba, E., Siahaan, B., & Sembiring, R. (2017). Collaborative Encryption Algorithm Between Vigenere Cipher, Rotation of Matrix (ROM), and One Time Pad (OTP) Algoritma. *Technology and Engineering Systems Journal*, 13-21.

[9] Pardede, A., Manurung, H., & Filina, D. (2017). Algoritma Vigenere Cipher Dan Hill Cipher Dalam Aplikasi Keamanan Data Pada File Dokumen. *Jurnal Teknik Informatika Kaputama (JTIK)*, 26-33.

[10] R.H Sianipar. (2017). *Visual Basic.Net Untuk Programmer.* Yogyakarta: Andi Offset.